KM Life®
KELESHEK MURASY

Выдержка из политики информационной безопасности АО «КСЖ «KM Life»

ЦЕЛЬ ПОЛИТИКИ

Предотвращение потерь конфиденциальности, целостности и доступности защищаемых активов, принадлежащих АО «КСЖ «KM Life» (далее — Компания), путём создания и поддержки системы управления информационной безопасностью (СУИБ), соответствующей требованиям законодательства Республики Казахстан и международным стандартам.

ОСНОВНЫЕ ЗАДАЧИ СУИБ

1) минимизировать ущерб, связанный с информационными рисками;
2) обеспечивать непрерывность ключевых бизнес-процессов;
3) предотвращать уничтожение имущества и ценностей;
4) предотвращать утечку, разглашение и несанкционированный доступ к конфиденциальной информации;
5) предотвращать сбои в работе технических средств, включая средства информатизации.
6) оперативно ликвидировать последствия нарушений ИБ.

КЛЮЧЕВЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СУИБ ПРИНЯТЫЕ В КОМПАНИИ

1. Законность – действия по ИБ основаны на законах РК и внутренних нормативных документах Компании, используя все разрешенные способы защиты информации;
2. Ориентированность на бизнес – меры ИБ поддерживают бизнес-цели Компании, не создавая препятствий для её деятельности;
3. Непрерывность – обеспечение ИБ проводится без остановок, гарантируя бесперебойную работу бизнес-процессов;
4. Комплексность – защита охватывает все аспекты жизни информационных ресурсов, на всех этапах их использования;
5. Обоснованность и экономическая целесообразность - средства защиты соответствуют уровню угроз и не превышают потенциальный ущерб от рисков;
6. Приоритетность – информационные ресурсы ранжируются по важности для определения уровня необходимой защиты;
7. Необходимое знание и наименьший уровень привилегий – доступ к данным ограничивается необходимым минимумом для выполнения работы;
8. Специализация – специалисты, ответственные за ИБ, должны иметь соответствующую квалификацию;
9. Информированность и персональная ответственность – работники осведомлены о правилах ИБ и несут ответственность за их соблюдение;
10. Координация – действия по ИБ координируются между подразделениями и с внешними организациями для эффективной защиты;

11. Подтверждаемость – все меры и процессы обеспечения ИБ должны быть задокументированы, чтобы иметь возможность их проверки, аудита и восстановления в случае необходимости;
12. Адаптивность и актуальность - система ИБ должна быть гибкой, позволяя оперативно адаптироваться к меняющимся внешним и внутренним угрозам, а также к развитию технологий и бизнес-процессов.

Основные объекты защиты (активы), включая материальные и нематериальные объекты, связанные с информационными технологиями и содержащие важную для Компании информацию:

- информационные ресурсы;
- программное обеспечение;
- телекоммуникационные средства и каналы связи;
- аппаратные средства.

КОНТРОЛЬ ДОСТУПА

Процедуры предоставления и управления доступом к информации регламентируются нормативно-технической документацией по обеспечению ИБ. В Компании определены и задокументированы процедуры регистрации и снятия с регистрации пользователей в отношении предоставления доступа к информационным ресурсам, сервисам сети и ИС Компании, в том числе в части предоставления привилегированных прав доступа.

ОБУЧЕНИЕ ПЕРСОНАЛА ПО ИБ

Все работники, стажеры и практиканты Компании проходят обязательное обучение или инструктаж по ИБ до предоставления доступа к электронным информационным ресурсам Компании. Обучение обеспечивает:

1) знание требований ИБ Компании;
2) умение безопасно использовать средства обработки информации и оборудование;
3) понимание порядка действий в случае инцидентов и внештатных ситуаций;
4) осведомленность о дисциплинарной ответственности и мерах, предусмотренных законодательством за нарушение требований ИБ.

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИБ

В целях своевременного выявления и оперативного реагирования на инциденты ИБ в Компании внедрена и поддерживается в актуальном состоянии система управления инцидентами ИБ, которая предусматривает определение и документирование процедур по выявлению, оценке и реагированию на инциденты ИБ. Компания обеспечивает ознакомление работников и подрядчиков с процедурами информирования об инцидентах нарушения ИБ, действующими в Компании.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (ИИ)

В целях повышения эффективности управления инцидентами ИБ в компании могут использоваться системы ИИ, при этом их работа должна контролироваться. Все решения ИИ подлежат логированию и проверке ответственными работниками, исключается передача критически важной, конфиденциальной или персональной информации, если это не предусмотрено политиками безопасности.

Согласовано:

Начальник Отдела по информационной и кибербезопасности	Б. Аллаяров	
Заместитель председателя Правления по правовым вопросам – член Правления	А. Тлемисова	
Заместитель председателя Правления по административному обеспечению – член Правления	О. Син	
Управляющий директор по информационным технологиям	М. Сергеев	
Начальник Службы управления рисками	М. Дя	
Начальник Службы комплаенс	А. Кембаева	
Начальник Отдела по общей безопасности	К. Калмаганбетов	
Начальник Отдела управления персоналом	А. Сарыпбек	